\AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Sorin-Miguel Ghiorghe,

Defendant(s).

Case No. 2:24-mj-02797-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of May 9, 2024, in the county of Los Angeles in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1029(a)(3)	Possession of fifteen or more unauthorized access devices

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Jacqueline Cenan
Complainant's signature

Jacqueline Cenan, USSS SA
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: May 10, 2024

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

U.S. Magistrate Judge Alicia G. Rosenberg
Printed name and title

AUSA: Alexander Gorin x3190

AFFIDAVIT

I, Jacqueline Cenan, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant for Sorin-Miguel Ghiorghe ("GHIORGHE"), for a violation of 18 U.S.C. § 1029 (a)(3) (possession of fifteen or more unauthorized access devices).

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only, all amounts or sums are approximate, and all dates and times are on or about those indicated.

II. BACKGROUND OF AFFIANT

3. I am a Special Agent ("SA") with the United States Secret Service ("USSS") and have been so employed since March 2021. In this capacity, I am responsible for investigating violations of federal criminal laws relating to financial institution fraud, credit card fraud, bank fraud, cybercrimes, and identity theft. I am a graduate of the Criminal Investigator Training Program conducted at the Federal Law Enforcement

Training Center in Glynco, Georgia, as well as the USSS Special Agent Training Course in Beltsville, Maryland. I have received advanced training in financial and cybercrime investigations including the Basic Investigation of Computers and Electronic Crimes Program, Basic Network Intrusion Responder Training, and I have received continued education related to the investigation and prosecution of cybercrimes. I have participated in multiple investigations in connection with fraud and cybercrimes.

III. SUMMARY OF PROBABLE CAUSE

4. Between January 2023 and March 2024, the California Department of Social Services ("DSS") has detected more than $139 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. Much of this fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

5. On April 1 and 2, 2024, law enforcement conducted physical surveillance at various banks and ATM locations throughout Los Angeles County, including a U.S. Bank ATM terminal located at 9110 Tampa Avenue, Northridge, CA, 91324 ("US BANK ATM 1"), which was identified as one of the top ATM locations in Los Angeles for EBT fraud.

6. On April 1, 2024, law enforcement saw two individuals (later identified, and referred to herein as "Co-conspirator 1" and "Co-conspirator 2") make unauthorized fraudulent withdrawals at US BANK ATM 1 and leave in a vehicle (referred to as "Subject

Vehicle 1." Law enforcement followed Subject Vehicle 1 to the Palazzo East Apartments, 344 S. Hauser Blvd., Los Angeles CA (the apartment complex where Unit #217 - herein referred to as "Subject Premises 1" - is located); Co-Conspirator 1 got out of Subject Vehicle 1 and entered the gate to the apartments, and Co-Conspirator 2 drove away.

7. Bank of America surveillance video footage shows Co-Conspirator 1 installing skimming devices at two Bank of America ATMs on April 1, 2024, which Bank of America Diebold technicians[1] have since recovered from the ATMs. On April 2, 2024, Co-Conspirator 1 drove a vehicle (herein referred to as "Subject Vehicle 2") to multiple banks, and made rapid ATM withdrawals. Subject Vehicle 2 later entered an underground parking garage located at Subject Premises 1. The surveillance team witnessed Co-Conspirator 1 enter apartment Unit #217.

8. On April 3, 2024, from 12:00 a.m. to 3:00 a.m., vehicle tracker data showed Subject Vehicle 1 in the vicinity of a Wells Fargo Bank, U.S. Bank, and Bank of America, and then traveling back to Subject Premises 1. Surveillance video footage from a nearby location ("Subject Premises 2") showed Co-Conspirator 1 and Co-Conspirator 2 entered the Park La Brea Tower 37 elevator bank on April 3, 2024, at approximately 3:08 a.m. Co-Conspirator 1 and Co-Conspirator 2 were holding what appeared to be pinhole camera ATM panels in their hands.

---

[1] Bank of America Diebold technicians are Field Service Technicians responsible for the maintenance and repair of Diebold Nixdorf ATMs. They have access to the upper level compartment of the ATM.

Because Subject Premises 1 and Subject Premises 2 are about a 2-minute walk from one another, I believe Subject Vehicle 1 was likely parked at Subject Premises 1 and Co-Conspirator 1 and Co-Conspirator 2 then walked across the street to Subject Premises 2. According to the vehicle tracker data, Subject Vehicle 1 remained at Subject Premises 1 for approximately an hour and a half before traveling to multiple other bank branches.

9. On May 4, 2024, Bank of America surveillance footage shows Co-Conspirator 1 and Co-Conspirator 2 placing a side panel pinhole camera and a deep insert skimming device on a Bank of America ATM. Co-Conspirator 1 and Co-Conspirator 2 left the ATM in a silver Mercedes with the license plate ending in U90, which is registered to Co-Conspirator 1, the registered resident of Subject Premises 1.

10. Subject Premises 1 and Subject Premises 2 are locations that are frequented by Co-Conspirator 1 and Co-Conspirator 2 for periods of time immediately preceding and following their illicit cash-out activity and skimmer installation which, in my training and experience, indicate that they are residences that will contain skimming equipment, skimming proceeds, stolen victim information, and information related to co-conspirators.

11. On May 9, 2024, at approximately 6:00 a.m., federal agents executed a search warrant[2] on Subject Premises 1. After breaching the apartment, agents detained GHIORGHE, who was found

---

[2] This search warrant (Case No. 2:24-mj-02734-DUTY) was signed by the Honorable Karen Stevenson, U.S. Magistrate Judge on May 8, 2024 (the "May Warrant").

in one of the bedrooms of the apartment. Agents also found approximately 281 cards, two skimming devices, skimming equipment such as cables that connect a skimmer to a laptop for the purpose of data transfer, device-making equipment such as a magnetic stripe reader, a voltage detector, a digital multimeter, and handwritten notes with card and victim account information.

12. Of the 281 cards that were found in Subject Premises 1 on May 9, 2024, 59 of them were found either in the room where he was found and that room's closet. All of these 59 cards are cloned cards containing victim EBT or EDD account information. By analyzing the transaction history of the victim EBT accounts, I was able to identify fraudulent charges that repeated across multiple victim accounts, indicating that they were used in a cash-out incident by GHIORGHE. U.S. Bank surveillance video later confirmed that GHIORGHE had withdrawn cash using several of these accounts, including on January 1, 3, 5, and February 1, 2024, which included unauthorized withdrawals, or attempted withdrawals, from 17 different victim accounts for a total of $9,720 in actual or attempted loss. On May 9, 2024, when federal agents searched Subject Premises 1, they found what appeared to be the same sweatshirt that GHIORGHE was wearing during the February 1, 2024, fraudulent attempted cash withdrawal in the car parked in the assigned spot of Subject Premises 1.

IV. STATEMENT OF PROBABLE CAUSE

13. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh and CalWORKs Programs

14. DSS is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

15. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

16. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a

grocery or convenient store by swiping the card at a point-of-sale terminal.

17. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

18. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

19. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

B. Background on EBT Fraud in the Los Angeles Area and Prior State and Federal Operations

20. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement

determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

21. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

22. On a legitimate debit or credit card, the information coded on the card's magnetic stripe will match the information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information coded on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be coded with the EBT card information, but the card itself will still bear the information of the gift card or bear no information if it is a blank white plastic card.

23. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested

to clone cards is often obtained from what is colloquially referred to as "skimming activity."

24. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

25. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

26. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period

of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

27. As a result of this operation, local law enforcement established surveillance at select ATMs that were used to conduct a significant volume of EBT fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of EBT benefits. As a result, law enforcement arrested approximately 16 suspects. All of the arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

28. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud

ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than $190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than $70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants were determined to be citizens Romania, who did not have documentation to be lawfully present in the United States. The three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. § 1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

29. In or about March 2023, federal law enforcement conducted another surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed

at select high-volume EBT fraud ATMs. Law enforcement arrested eleven suspects that conducted a high volume of unauthorized transactions and that conducted those transactions in rapid succession. At the time of their arrest, the suspects had in their possession over 400 cloned cards, $120,000 in illicitly obtained funds, and multiple skimming devices.

30. Ten out of the eleven of these defendants were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States.

C. Background of Current Operation to Combat EBT Fraud

31. Data provided by DSS, based in part upon reported fraud by victims, reported fraud to local law enforcement, bank records, and surveillance indicates that as of in or about March 2024, there has been over $139 million in stolen funds from victim EBT cards.

32. Between January 1, 2024 and March 1, 2024, more than $18.1 million has been stolen from victim EBT cards. Of the approximately $18.1 million stolen, approximately $5.5 million has been stolen from victim EBT cards in Los Angeles County alone. The majority of these funds were stolen through unauthorized ATM withdrawals.

33. Between on or about February 1, 2024, and on or about February 5, 2024, more than $8.2 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately $8.2 million stolen from victim EBT cards in the beginning of February 2024, more than $2.7 million was stolen,

almost entirely through unauthorized ATM withdrawals, in Los Angeles County alone.

34. For example, between on or about February 1, 2024, and on or about February 5, 2024 more than $117,000 was withdrawn from ATMs at a single financial institution branch located in Los Angeles, California in Los Angeles County. The unauthorized withdrawals conducted during these five days and at this single bank branch affected approximately 156 victim EBT cardholders. The dates of these withdrawals coincided with the disbursement by DSS of EBT benefits, including CalFresh and CalWORKs.

35. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because benefits are typically disbursed to EBT cardholders during the early days of each month.

36. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding

stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

37. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

1. Co-Conspirator 1 and Co-Conspirator 2 Committed EBT Fraud Using Unauthorized Access Devices on April 1, 2024

38. On April 1, law enforcement conducted physical surveillance at various banks and ATM locations throughout Los Angeles County, including US BANK ATM 1, which was identified as one of the top ATM locations in Los Angeles for EBT fraud.

39. On April 1, 2024, at approximately 5:50 a.m., based on my conversation with other law enforcement agents, law enforcement observed Subject Vehicle 1 park in the US BANK ATM 1 parking lot. At approximately 6:00 a.m. a male passenger, later identified as Co-Conspirator 1, exited Subject Vehicle 1 and approached the US BANK ATM 1 walk up terminal. Law enforcement observed Co-Conspirator 1 make what appeared to be rapid cash withdrawals with multiple cards. Law enforcement observed, and

U.S. Bank confirmed, that Co-Conspirator 1 used 25 different EBT cards to withdraw approximately $24,540.

40. At the same time that Co-Conspirator 1 made transactions at the US BANK ATM 1 walk up terminal, based on my conversation with other law enforcement agents, law enforcement observed Subject Vehicle 1 pull into the drive-through ATM. Law enforcement observed, and bank surveillance confirmed, that an individual later identified as Co-Conspirator 2 used 27 different EBT cards to withdraw approximately $24,940.00.

41. Based on my conversation with other law enforcement agents, law enforcement observed Co-Conspirator 1 walk back to Subject Vehicle 1 and both he and Co-Conspirator 2 exited the parking lot in Subject Vehicle 1. Law enforcement began mobile surveillance of Subject Vehicle 1.

42. Based on my conversation with other law enforcement agents, after leaving the U.S. Bank parking lot, law enforcement observed Subject Vehicle 1 conduct multiple countersurveillance measures in order to evade law enforcement surveillance, such as making multiple unnecessary right turns in a row before starting its route to its next destination.

43. Based on my conversation with other law enforcement agents, during the surveillance, at approximately 6:50 a.m., law enforcement observed Subject Vehicle 1 stop at a Bank of America located at 18337 Ventura Blvd. Tarzana, CA ("BANK OF AMERICA ATM 1") before driving to the Palazzo East Apartments, located at 344 Hauser Blvd., Los Angeles CA (the apartment complex where Subject Premises 1 is located), where law enforcement observed

Co-Conspirator 1 get out of Subject Vehicle 1. Law enforcement observed Co-Conspirator 1 enter the gate to the apartments. Law enforcement then observed Co-Conspirator 2 drive away in Subject Vehicle 1.

44. Based on my conversation with other law enforcement agents, the surveillance team continued to follow Co-Conspirator 2 in Subject Vehicle 1. The surveillance team then placed a vehicle tracker on Subject Vehicle 1 at 7:50 a.m.[3]

45. According to the vehicle tracker data, later that day, on April 1, 2024, at approximately 2:51 p.m., Subject Vehicle 1 drove to 400 S. Burnside Ave, Los Angeles, CA 90036 (the apartment complex where Subject Premises 2 is located) and parked in the apartment complex's parking lot for approximately thirty minutes. According to the vehicle tracker data, at approximately 3:23 p.m., Subject Vehicle 1 departed from Subject Premises 2 and proceeded to spend all night driving to different bank branches.

46. On April 1, 2024, at approximately 4:20 p.m., vehicle tracker data shows that Subject Vehicle 1 was in the parking lot of the Bank of America located at 11990 Garvey Ave, El Monte CA ("BANK OF AMERICA ATM 2"). Between 4:19 p.m. and 5:09 p.m., Co-Conspirator 1 can be seen on Bank of America surveillance video opening BANK OF AMERICA ATM 2 and installing a skimming device. Subject Vehicle 2 can be seen in the background of the bank surveillance. Based on my training and experience, while Co-

---

[3] The tracker was placed on Subject Vehicle 1 pursuant to a tracker warrant (2:24-MJ-01847) signed by Honorable Charles F. Eick, U.S. Magistrate Judge.

Conspirator 1 installed the skimming device and used Subject Vehicle 2 as his "tech van," Co-Conspirator 2 was conducting countersurveillance in Subject Vehicle 1.

47. On April 8, 2024, a Bank of America Diebold technician checked the BANK OF AMERICA ATM 2 that was visited by Co-Conspirator 1 and Co-Conspirator 2 on April 1, 2024, and he found a skimming device. Bank of America turned over the skimming device to law enforcement to preserve as evidence.

48. On April 1, 2024, from approximately 7:39 p.m. to 8:33 p.m., vehicle tracker data shows that Subject Vehicle 1 was in the parking lot of the Bank of America located at BANK OF AMERICA ATM 1. Between 7:37 p.m. and 8:26 p.m., Bank of America surveillance footage from BANK OF AMERICA ATM 1 shows Co-Conspirator 1 driving Subject Vehicle 2 through a drive-through ATM, opening the ATM, and installing a skimming device. In the surveillance footage, based on my training and experience, Co-Conspirator 1 can be seen impersonating an ATM technician by placing a traffic cone behind his vehicle in order to dissuade customers from disturbing his work. Based on my training and experience, while Co-Conspirator 1 installed the skimming device and used Subject Vehicle 2 as his "tech van," Co-Conspirator 2 was conducting countersurveillance in Subject Vehicle 1.

49. On April 8, 2024, a Bank of America Diebold technician checked the Bank of America ATM located at BANK OF AMERICA ATM 1 that was visited by Co-Conspirator 1 and Co-Conspirator 2 on April 1, 2024, and he found a skimming device.

Bank of America turned over the skimming device to law enforcement to preserve as evidence.

50. Based on my conversation with other law enforcement agents and my own review of Bank of America surveillance footage, Bank of America surveillance footage reveals that Co-Conspirator 1 is using a key to open Bank of America Diebold ATMs. Once the ATMs are open, Bank of America surveillance footage shows Co-Conspirator 1 installing skimming devices. In the Bank of America surveillance footage, Co-Conspirator 1 can be seen wearing a lanyard around his neck, driving a white van (that looks like the white van that Diebold technicians drive), which based on my training and experience, Co-Conspirator 1 is doing in order to impersonate ATM technicians and appear less suspicious while he is installing skimming devices. While Co-Conspirator 1 is manipulating the ATM, Co-Conspirator 2 can be seen in the Bank of America surveillance footage helping Co-Conspirator 1 install/remove skimming devices by bringing him skimming equipment. Additionally, vehicle tracker data shows Subject Vehicle 1 driving around the parking lot, which based on my training and experience, appears to be a countersurveillance measure used to detect law enforcement. Bank of America has confirmed that neither Co-Conspirator 1 nor Co-Conspirator 2 work for the bank, and they should not have access to the inner compartments of the ATM.

51. According to vehicle tracker data, after installing skimming devices at BANK OF AMERICA ATM 1 and BANK OF AMERICA

ATM 2, on April 1, 2024, the Subject Vehicle 1 returned to Subject Premises 2 at 9:05 p.m.

52. That same day, on April 1, 2024, at 10:26 p.m., vehicle tracker data indicates that Subject Vehicle 1 left Subject Premises 2 and spent the rest of the night and the next morning driving to different bank branches (i.e., one Wells Fargo Bank, three Bank of America branches, and one U.S. Bank Branch), before returning to Subject Premises 2 at 4:30 a.m. on April 2, 2024.

2. Co-Conspirator 1 Committed EBT Fraud Using Unauthorized Access Devices on April 2, 2024

53. On April 2, 2024, at 5:18 a.m., vehicle tracker data indicates that Subject Vehicle 1 traveled from Subject Premises 2 to a Wescom Credit Union, a Wells Fargo, and a US Bank Branch.

54. Based on my conversation with law enforcement agents, on April 2, 2024, at approximately 6:00 a.m., law enforcement observed Subject Vehicle 2 pull up to the US BANK ATM 1 drive through terminal. Law enforcement, with the help of bank surveillance footage, confirmed that the driver of Subject Vehicle 2 was Co-Conspirator 1. Law enforcement observed Co-Conspirator 1 making rapid ATM withdrawals and appeared to place the cash inside the vehicle. Law enforcement observed, and U.S. Bank confirmed, that Co-Conspirator 1 used 10 different EBT cards to withdraw approximately $8,940 from the US BANK ATM 1 drive through terminal.

55. Based on my conversation with law enforcement agents, at approximately 6:15 a.m., law enforcement observed Co-

Conspirator 1 leave US BANK ATM 1 driving Subject Vehicle 2 and law enforcement commenced mobile surveillance. Similar to Subject Vehicle 1, law enforcement observed Subject Vehicle 2 display countersurveillance measures after it left the US BANK ATM 1 parking lot by making multiple unnecessary right turns. Law enforcement also observed Subject Vehicle 2 briefly enter an empty parking lot, which in my training and experience, is a tactic that criminals will use in order to expose any individuals that might be following them.

56. After leaving the US BANK ATM 1 parking lot, based on my conversation with law enforcement agents, law enforcement observed Subject Vehicle 2 enter a Chase Bank ATM parking lot located at 19315 Saticoy Street, Reseda, CA 91335. Law enforcement was unable to observe any transactions at this location but did observe Co-Conspirator 1 re-enter Subject Vehicle 2 and exit the parking lot. Law enforcement continued mobile surveillance.

57. Based on my conversation with law enforcement agents, at approximately 6:30 a.m., law enforcement observed Co-Conspirator 1 park Subject Vehicle 2 and approach another U.S. Bank ATM located at 19500 Ventura Boulevard, Tarzana, CA, 91356 ("US BANK ATM 2"). Law enforcement observed Co-Conspirator 1 conduct multiple rapid transactions and retrieve what appeared to be currency at the conclusion of each transaction and place the currency in a jacket pocket. U.S. Bank confirmed Co-Conspirator 1 utilized approximately 7 different EBT cards and withdrew a total of approximately $8,120. Law enforcement

observed Co-Conspirator 1 enter Subject Vehicle 2 and drive away.

58. Based on my conversation with law enforcement agents, at approximately 6:45 a.m., law enforcement observed Co-Conspirator 1 exit Subject Vehicle 2 at another U.S. Bank located at 17250 Ventura Boulevard, Encino, CA 91316 ("US BANK ATM 3"). Law enforcement observed Co-Conspirator 1 approach US BANK ATM 3 and conduct multiple transactions for approximately 40 minutes. U.S. Bank confirmed Co-Conspirator 1 used a total of 32 separate EBT cards to withdraw an approximate total of $18,580 and attempted a total withdrawal of $24,020. At 7:20 a.m., law enforcement observed Co-Conspirator 1 leave US BANK ATM 3, enter Subject Vehicle 2, and drive away.

59. Based on my conversation with law enforcement agents, law enforcement continued surveillance and observed Subject Vehicle 2 enter an underground parking garage located at Subject Premises 1. Subject Premises 1 is the same location Co-Conspirator 1 was dropped off by Co-Conspirator 2 in Subject Vehicle 1 the day prior. The surveillance team saw Co-Conspirator 1 enter apartment Unit #217 and later found Subject Vehicle 2 in parking spot #92. At approximately 2:00 p.m. a vehicle tracker was authorized, placed, and installed on Subject Vehicle 2.[4]

60. I learned in the course of this investigation that Palazzo Apartments unit 217 has assigned parking spots #92 and

---

[4] The tracker was placed on Subject Vehicle 2 pursuant to a tracker warrant (2:24-MJ-01909) signed by Honorable Patricia Donahue, U.S. Magistrate Judge.

#93 and is registered to Individual A. The #217 unit has been registered to Individual A since April 2023.

61. Based on my training and experience, individuals that conduct unauthorized cash withdrawals using victim EBT accounts will amass large amounts of cash in a short amount of time, and they will usually take their large amounts of cash to a safe location (e.g., a residence, storage unit, etc.) immediately after finishing their cash-out activity because keeping it in the vehicle puts it at risk of being seen by law enforcement in the event of a traffic stop or stolen. Additionally, skimming suspects will often owe a percentage of the total amount of cash they made to the individual or group that sold them their cloned cards, so the residence may belong to other skimming suspects. Based on my conversation with law enforcement agents, law enforcement observed Co-Conspirator 1 going to Subject Premises 1 after doing a large number of unauthorized cash-outs on April 1 and April 2, 2024 and then, after leaving Subject Premises 1 on April 2, 2024, he went to multiple bank branches to install skimming devices.

3. Video Surveillance Shows Co-Conspirator 1 Installing a Skimming Device on April 2, 2024

62. Based on my conversation with law enforcement agents, on April 2, 2024, at approximately 8:53 p.m., vehicle tracker data showed that Subject Vehicle 2 had left Subject Premises 1 and had traveled to a Bank of America ATM located at 14310 Hawthorne Blvd, Lawndale CA 90260 ("BANK OF AMERICA ATM 3"). According to the vehicle tracker data, Subject Vehicle 1 and

Subject Vehicle 2 were in the parking lot of the BANK OF AMERICA ATM 3 between approximately 9:00 and 9:40 p.m. Bank of America surveillance during that time frame shows Co-Conspirator 1 inspecting the ATM, testing the ATM card reader by inserting a card, opening the ATM, installing a device that appears to be a skimming device with tools like tape and a screwdriver, closing the ATM, and inserting another card, before returning to Subject Vehicle 2 and driving out of the parking lot.According to vehicle tracker data, after leaving the parking lot, Subject Vehicle 1 and Subject Vehicle 2 traveled to another Bank of America ATM located at 1957 Pacific Coast Hwy, Lomita CA, 90717 ("BANK OF AMERICA ATM 4"). Bank of America surveillance from April 2, 2024, 9:49 p.m. to 10:11 p.m., shows Subject Vehicle 2 in the parking lot of the Bank of America ATM and Co-Conspirator 1 opening the ATM and inserting what appears to be a skimming device, before closing the ATM and returning to Subject Vehicle 2.On April 8, 2024, Bank of America Diebold technicians physically inspected the inside of the BANK OF AMERICA ATM 4 and found a skimming device. Bank of America turned the skimming device over to law enforcement in order for it to preserved as evidence.

63. According to vehicle tracker data, after leaving the BANK OF AMERICA ATM 4 parking lot, Subject Vehicle 1 and Subject Vehicle 2 traveled back to Subject Premises 2.

64. That same night, according to vehicle tracker data, Subject Vehicle 1 only remained at Subject Premises 2 for

approximately 30 minutes before leaving at 11:30 p.m. to multiple bank branches.

4. Video Surveillance Shows Co-Conspirator 2 Holding Skimming Equipment on April 3, 2024

65. On April 3, 2024, from approximately midnight to 3:00 a.m., the vehicle tracker data shows Subject Vehicle 1 in the vicinity of a Wells Fargo Bank, U.S. Bank, and Bank of America. The vehicle tracker data shows Subject Vehicle 1 then traveled to Subject Premises 1.

66. Later that morning, on April 3, 2024, vehicle tracker data shows Subject Vehicle 1 traveled to a Bank of America located at 20461 Leapwood Ave, Carson CA ("BANK OF AMERICA ATM 5"). Vehicle tracker data and Bank of America surveillance show Subject Vehicle 1 at the BANK OF AMERICA ATM 5 from 5:26 a.m. to 5:37 a.m. and from 6:51 a.m. to 7:15 a.m. Bank of America surveillance shows Co-Conspirator 2 and Co-Conspirator 1 at the BANK OF AMERICA ATM 5 at those times and Co-Conspirator 2 is holding what appears to be skimming equipment.

67. On April 8, 2024, a Bank of America Diebold technician physically inspected the BANK OF AMERICA ATM 5 and found a skimming device. The skimming device was turned over to law enforcement to be preserved as evidence.

68. After installing a skimming device at the BANK OF AMERICA ATM 5, vehicle tracker data shows Subject Vehicle 1 traveled to two different Wells Fargo branches and one U.S. Bank branch, before arriving in the parking lot of Subject Premises 2 at approximately 9:25 a.m., on April 3, 2024.

At approximately 9:28 a.m., on April 3, 2024, surveillance video provided to law enforcement by the Park La Brea Security Team shows Co-Conspirator 1 enter the Tower 37 elevator bank. By analyzing the access fob swipe record, the Park La Brea security team was able to identify that the unit associated with the fob that was swiped by Co-Conspirator 1 is unit 37-11D (i.e., Subject Premises 2).

5. Video Surveillance Shows Co-Conspirator 1 Holding Skimming Equipment On April 4, 2024

69. On April 2, 2024, from 3:43 a.m. to 4:01 a.m., vehicle tracker data shows Subject Vehicle 1 in the parking lot of the U.S. Bank located at 3645 E Imperial Hwy, Lynwood, CA ("US BANK ATM 4"). On April 3, 2024, from 2:03 a.m. to 2:09 a.m., vehicle tracker data shows Subject Vehicle 1 in the parking lot of the US BANK ATM 4. On April 4, 2024, from approximately 10:17 to 10:19 p.m., U.S. Bank surveillance footage shows Co-Conspirator 1 installing a skimming device at the US BANK ATM 4.

70. On April 4, 2024, U.S. Bank representatives manually inspected the U.S. BANK ATM 4 that was visited by Co-Conspirator 1 and found a skimming device. U.S. Bank mailed the skimming device to law enforcement to be preserved as evidence.

71. After being alerted by law enforcement of the skimming activity taking place at their bank location, U.S. Bank physically inspected US BANK ATM 4 on April 5, 2024 and found another skimming device, which was turned over to law enforcement as evidence.

72. On April 4, 2024, from midnight to 1:17 a.m., vehicle tracker data shows that Subject Vehicle 1 drove to a Bank of America located at 242 Towne Center Dr, Compton, CA 90220 ("BANK OF AMERICA ATM 6"), a U.S. Bank branch, a Wells Fargo bank branch, and a Chase bank branch, before returning to Subject Premises 2 at approximately 1:18 a.m.

From approximately 12:26 a.m. to 12:37 a.m., Bank of America surveillance footage shows Co-Conspirator 1 and Co-Conspirator 2 at BANK OF AMERICA ATM 6, manipulating the physical components of the ATM's inner compartment and holding skimming equipment.

73. At approximately 1:18 a.m., on April 4, 2024, surveillance video provided to law enforcement by the Park La Brea Security Team shows Co-Conspirator 2 enter the Tower 37 mail room. By analyzing the access fob swipe record, the Park La Brea security team was able to identify that the unit associated with the fob that was swiped by Co-Conspirator 2 is unit 37-11D (i.e., Subject Premises 2).

74. Subject Premises 1 and Subject Premises 2 are locations that are frequented by Co-Conspirator 1 and Co-Conspirator 2 for periods of time immediately preceding and following their illicit cash-out activity and skimmer installation.

6. Video Surveillance Shows Co-Conspirator 1 and Co-Conspirator 2 Inserting a Skimming Device on May 4, 2024

75. On May 2, 2024, at approximately 12:32 a.m., according to Bank of America surveillance footage, two unknown suspects drove a white SUV through the drive-through of BANK OF AMERICA

ATM 1 in Tarzana, California. These two suspects installed two overlay skimming devices on the ATMs located in the drive through. At 12:34 a.m., an unknown suspect in a black BMW with the license plate ending in 904 checked the ATM's functioning and overlays.

76. On May 3, 2024, at approximately 12:50 a.m., law enforcement observed this black BMW with license plate ending in 904 drive into parking lot E of Subject Premises 2 and park in the parking spot 93, which belongs to Subject Premises 2.

77. On May 4, 2024, at approximately 03:43 a.m., Co-Conspirator 1 and Co-Conspirator 2 can be seen in Bank of America surveillance footage placing a side panel pinhole camera and a deep insert skimming device on BANK OF AMERICA ATM 6. According to Bank of America video surveillance, Co-Conspirator 1 and Co-Conspirator 2 left BANK OF AMERICA ATM 6 in the silver Mercedes with license plate ending in U90. This vehicle is registered to Individual A, the registered resident of Subject Premises 1.

78. On May 6, 2024, at approximately 12:48 p.m., law enforcement observed a blue Mercedes with the license plate ending in 020 parked in spot 93 of Subject Premises 1. This vehicle is registered to Individual B and 400 S Burnside Ave, 11D (i.e., Subject Premises 2).

79. Based on my review of domestic and international law enforcement database records, Co-Conspirator 1 has an extensive criminal history. In 2021, Co-Conspirator 1 was sentenced to 1 year in prison for counterfeiting documents in Hungary. In 2017,

Co-Conspirator 1 was sentenced to 5 years in prison for theft, computer fraud, and organized crime in Belgium. In 2012, Co-Conspirator 1 was sentenced to 8 months in prison for aggravated identity theft in France. In 2005, Co-Conspirator 1 was sentenced to 15 months in prison for theft, forgery of documents, and computer fraud in Germany. In 2004, Co-Conspirator 1 was sentenced to 6 months in prison for theft in Austria. In 2003, Co-Conspirator 1 was sentenced to 2 years in prison for theft in Bulgaria. In 2003, Co-Conspirator 1 was sentenced for theft in Romania, but he was later rehabilitated.

80. In 2021, Co-Conspirator 2 was sentenced to 1 year in prison (suspended sentence) for counterfeiting documents in Hungary. In 2019, Co-Conspirator 2 was sentenced to 18 months for creation of an organized crime group and illegal operations with devices or software in Romania. In 2013, Co-Conspirator 2 was sentenced to 1 year for indecent exposure in Romania and to 20 days in prison for theft in Belgium. In 2011, Co-Conspirator 2 was sentenced to 6 months in prison for theft in France. In 2008, Co-Conspirator 2 was sentenced to 10 months for theft in Norway. In 2007, Co-Conspirator 2 was sentenced to 20 days in prison for theft in Norway.

81. Based on my review of domestic and international law enforcement database records, in 2016, Co-Conspirator 2 was convicted in the Washington County District Court of Aggravated Identity Theft and was sentenced to 24 months in prison, Second Degree Burglary and was sentenced to 6 months in prison, and Identity Theft and was sentenced to 6 months in prison.

82. On February 2, 2024, LAPD obtained a warrant for Co-Conspirator 2 arrest for Burglary.

83. ICE further confirmed that Co-Conspirator 2 and Co-Conspirator 1 have no lawful presence in the United States.

7. May 9, 2024 Search of Subject Premises 1 Finds GHIORGHE Along With Unauthorized Access Devices, Skimming Devices, and Skimming Equipment

84. On May 8, 2024, federal search warrants were signed for Subject Premises 1 and Subject Premises 2. On May 9, 2024, at approximately 6:00 a.m., federal agents executed the May Warrant on Subject Premises 1. After entering the apartment, agents found GHIORGHE in one of the apartment's bedrooms and detained GHIORGHE. Agents also found approximately 281 cards, two skimming devices, skimming equipment such as cables that connect a skimmer to a laptop for the purpose of data transfer, device-making equipment such as a magnetic stripe reader, a voltage detector, a digital multimeter, and handwritten notes with card and victim account information.

85. Agents also found a Romanian identification card, Romanian passport, and Romanian driver's license with GHIORGHE's name and face. Based on information provided by ICE, GHIORGHE has no lawful presence in the United States and entered the country illegally through Chula Vista, San Diego on October 6, 2023.

86. At approximately 7:30 a.m., I read GHIORGHE his Miranda Rights in Romanian. GHIORGHE acknowledged that he understood his rights and wanted to speak to me. GHIORGHE stated that he lives in the apartment by himself and that he moved here

from Romania two months ago. GHIORGHE stated that all of the phones found in his room belong to him and provided the passcode to the phones found in his bedroom. When asked why he has cloned cards in his apartment, GHIORGHE stated that he did not know where they came from, that the cards and the skimming equipment just appeared in his apartment about a week ago. GHIORGHE stated that he has never done cash-outs at the ATM using cards containing other people's information.

87. Of the 281 cards that were found in GHIORGHE's residence on May 9, 2024, 59 of them were found either in the room he identified as his or his closet. Based on information from United States Department of Agriculture OIG, 32 of the 59 cards found in GHIORGHE's bedroom and closet are cloned cards containing victim EBT account information. Based on my training and experience concerning bank identification numbers, an additional 26 cloned cards found in GHIORGHE's bedroom and closet are cloned cards likely containing victim EDD account information. By analyzing the transaction history of the victim EBT accounts, I was able to identify fraudulent charges that repeated across multiple victim accounts, indicating that they were used in a cash-out incident by GHIORGHE. This was later confirmed by U.S. Bank surveillance video which was provided to law enforcement.

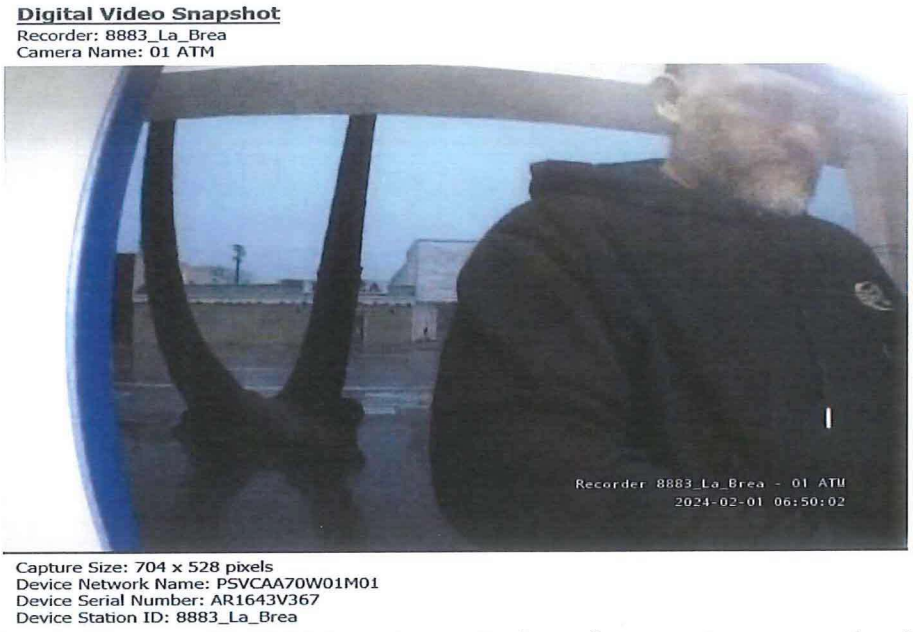
88. For example, on January 1, 2024, from approximately 6:15 a.m. to 6:20 a.m., GHIORGHE and an unknown suspect can be seen on bank surveillance video (see below) at a U.S. Bank ATM located at 3605 S La Brea Ave, Los Angeles, CA 90016 ("US BANK

ATM 5") conducting unauthorized withdrawals using four different victim EBT accounts to withdraw $2080.00. All four of these EBT accounts were found on cloned cards in the Hauser residence at the time of the warrant's execution.

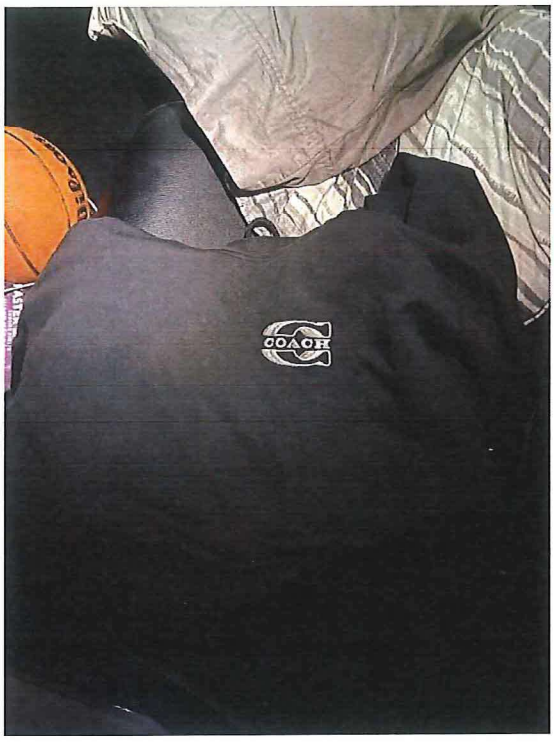
89. On January 3, 2024, from approximately 6:00 to 6:10 a.m., GHIORGHE can be seen on bank surveillance video (see below) at a US Bank ATM 5 conducting unauthorized withdrawals using nine different victim EBT accounts to withdraw $6,980.00. Eight out of the nine of these EBT accounts were found on cloned cards in GHIORGHE's bedroom or closet in the Hauser residence at the time of the May Warrant's execution.

90. On January 5, 2024, from approximately 7:05 a.m. to 7:07 a.m., GHIORGHE can be seen on bank surveillance video at a US Bank ATM 5 conducting unauthorized withdrawals using three different victim EBT accounts to attempt to withdraw $660.00. All three of these transactions were denied. All three of these EBT accounts were found on cloned cards in the Hauser residence at the time of the May Warrant's execution.

91. On February 1, 2024, at approximately 6:50 a.m., GHIORGHE can be seen on bank surveillance video at a U.S. Bank ATM located at 736 N La Brea Ave, Los Angeles, CA 90038 ("US BANK ATM 6") wearing a black "COACH" sweatshirt and attempting to conduct an unauthorized withdrawal using the EBT account ending in 6941. The transaction failed due to an incorrect PIN. This EBT account was found on a cloned card in GHIORGHE's room or closet in the Hauser residence at the time of the MAY Warrant's execution.



92. On May 9, 2024, when federal agents searched Subject Premises 1, agents located a black sweatshirt that appears to be the sweatshirt GHIORGHE was wearing in the cash-out incident pictured above in the backseat of the vehicle parked in the space assigned to Unit #217 (which the May Warrant authorized agents to search).



V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

93. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their

digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars or homes.

VI. CONCLUSION

94. For all of the reasons described above, there is probable cause to believe that GHIORGHE has committed a violation of 18 U.S.C. § 1029 (a)(3) (possession of fifteen or more access devices).

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 10th day of May, 2024.

Alicia G. Rosenberg

THE HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE